IOS Crash Log

&

Sysdiagnose Log

Aung Zaw Myo

Crash Log

Crash Log ကိုတော့ System ဒါမှမဟုတ် Application Crash ဖြစ်တဲ့အခါမှာ IOS System ကနေ Crash Log အနေနဲ့ Automatic ထုတ်ပေးပါတယ်။ Crash Log နဲ့ပတ်သတ်ပြီး အသေးစိတ်သိချင်တယ်ဆိုရင် Apple ကနေ Developer တွေအတွက် ဖော်ပြထားတဲ့ Crash Log မှာ အသေးစိတ်ကြည့်နိုင်ပါတယ်။ Device မှာ Crash Log ကိုသိမ်းဆည်းထားတဲ့နေရာကတော့

/private/var/mobile/Library/Logs/CrashReporter/

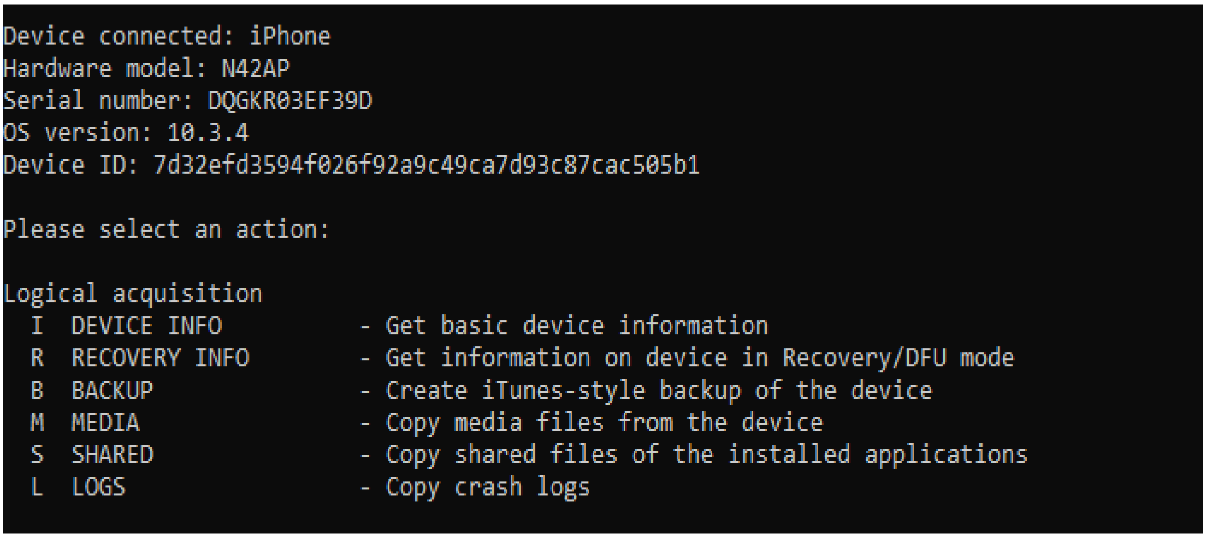
/private/var/root/Library/Logs/CrashReporter/

Crash Log ကို အချို့သော Mobile Forensics Tools တွေမှာ Logical Extraction ရယူရင်ပါဝင်ပါတယ်။ အချို့သော Mobile Forensics Tools တွေမှာ တော့မပါဝင်တတ်ပါဘူး။ မပါဝင်တဲ့အခါမှာ Crash Log ကိုသီးသန့်ထုတ် ယူပြီး ကြည့်နိုင်ပါတယ်။ ဘယ်အချိန်တွေမှာရယူသလဲဆိုရင် Device ကနေရနိုင်သမျှ Information တွေကိုရယူလိုတဲ့အခါ။ Crash Log ကိုပဲရယူနိုင်တဲ့ အခြေအနေ။ Case အရ Log File ကို ရယူရမဲ့အခြေအနေတွေမှာ Log File ကိုရယူပါတယ်။ Crash Log မှာ User Information တွေဖြစ်တဲ့ Photo, Chat, Message, Call Log စတာတွေ မပါဝင်ပါဘူး။ Device မှာ Install ပြုလုပ်ထားတဲ့ App တွေရဲ့ Execution Time တွေ Wireless Information တွေ ပါဝင်ပါတယ်။ Device မှာ Application ကို Uninstall လုပ်ခဲ့ရင်တောင် Log အနေနဲ့ ကျန်နေတတ်ပါတယ်။

Crash Log ကိုရယူနိုင်တဲ့နည်းလမ်းတွေကတော့ iTunes, libimobiledevice, IOS Device Manager Tools, Elcomsoft IOS Forensics Tools Kit, AirDrop, XCode, 3UTools စတာတွေနဲ့ရယူနိုင်ပါတယ်။ အခု PDF မှာတော့ libimobiledevice, Elcomsoft IOS Forensics Tools Kit, 3UTools နဲ့ရယူပါမယ်။ Elcomsoft IOS Forensics Tools Kit ကတော့ Commercial Tools ဖြစ်ပါတယ်။

Elcomsoft IOS Forensics Tools Kit

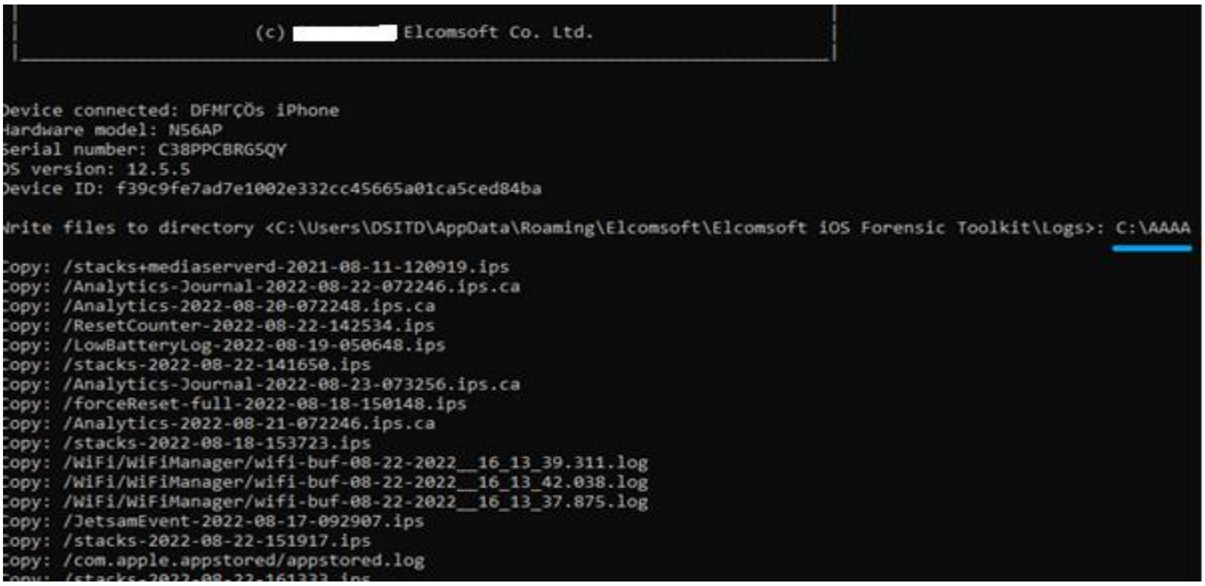
L – Command ကိုအသုံးပြုပြီး Crash Log ကိုရယူပါတယ်။ မျဉ်းတားထား တာကတော့ Crash Log ကိုသိမ်းဆည်းမည့်နေရာဖြစ်ပါတယ်။ Crash Log ကိုရယူဖို့အတွက် JailBreak ပြုလုပ်ဖို့မလိုအပ်ပါဘူး။ ကျွန်တော် အခုအသုံးပြုတဲ့ IPhone ဆိုရင် Activation Lock ပါကျနေပါတယ်။ ဒါကြောင့်အချို့နေရာတွေမှာ ရရှိနိုင်တဲ့ Result ကနည်းနေပါမယ်။



```
Device connected: iPhone
Hardware model: N42AP
Serial number: DQGKR03EF39D
OS version: 10.3.4
Device ID: 7d32efd3594f026f92a9c49ca7d93c87cac505b1

Please select an action:

Logical acquisition
  I   DEVICE INFO           - Get basic device information
  R   RECOVERY INFO         - Get information on device in Recovery/DFU mode
  B   BACKUP                - Create iTunes-style backup of the device
  M   MEDIA                 - Copy media files from the device
  S   SHARED                - Copy shared files of the installed applications
  L   LOGS                  - Copy crash logs
```



```
(c) [redacted] Elcomsoft Co. Ltd.

Device connected: DFMΓÇÖs iPhone
Hardware model: N56AP
Serial number: C38PPCBRGSQY
OS version: 12.5.5
Device ID: f39c9fe7ad7e1002e332cc45665a01ca5ced84ba

Write files to directory <C:\Users\DSITD\AppData\Roaming\Elcomsoft\Elcomsoft iOS Forensic Toolkit\Logs>: C:\AAAA

Copy: /stacks+mediaserverd-2021-08-11-120919.ips
Copy: /Analytics-Journal-2022-08-22-072246.ips.ca
Copy: /Analytics-2022-08-20-072248.ips.ca
Copy: /ResetCounter-2022-08-22-142534.ips
Copy: /LowBatteryLog-2022-08-19-050648.ips
Copy: /stacks-2022-08-22-141650.ips
Copy: /Analytics-Journal-2022-08-23-073256.ips.ca
Copy: /forceReset-full-2022-08-18-150148.ips
Copy: /Analytics-2022-08-21-072246.ips.ca
Copy: /stacks-2022-08-18-153723.ips
Copy: /WiFi/WiFiManager/wifi-buf-08-22-2022__16_13_39.311.log
Copy: /WiFi/WiFiManager/wifi-buf-08-22-2022__16_13_42.038.log
Copy: /WiFi/WiFiManager/wifi-buf-08-22-2022__16_13_37.875.log
Copy: /JetsamEvent-2022-08-17-092907.ips
Copy: /stacks-2022-08-22-151917.ips
Copy: /com.apple.appstored/appstored.log
```

Name	Date modified	Type	Size
Assistant	23-Aug-22 10:05 AM	File folder	
Baseband	23-Aug-22 10:05 AM	File folder	
com.apple.appstored	23-Aug-22 10:05 AM	File folder	
DiagnosticLogs	23-Aug-22 10:05 AM	File folder	
Retired	23-Aug-22 10:05 AM	File folder	
WiFi	23-Aug-22 10:05 AM	File folder	
Analytics-2022-08-17-092127.ips	23-Aug-22 10:05 AM	CA File	1 KB
Analytics-2022-08-18-081932.ips	23-Aug-22 10:05 AM	CA File	3 KB
Analytics-2022-08-19-092154.ips	23-Aug-22 10:05 AM	CA File	68 KB
Analytics-2022-08-20-072248.ips	23-Aug-22 10:05 AM	CA File	86 KB
Analytics-2022-08-21-072246.ips	23-Aug-22 10:05 AM	CA File	35 KB
Analytics-2022-08-22-072246.ips	23-Aug-22 10:05 AM	CA File	22 KB
Analytics-2022-08-23-073256.ips	23-Aug-22 10:05 AM	CA File	
Analytics-Journal-2022-08-17-092128.ips	23-Aug-22 10:05 AM	CA File	
Analytics-Journal-2022-08-18-081932.ips	23-Aug-22 10:05 AM	CA File	
Analytics-Journal-2022-08-19-092155.ips	23-Aug-22 10:05 AM	CA File	
Analytics-Journal-2022-08-20-072248.ips	23-Aug-22 10:05 AM	CA File	
Analytics-Journal-2022-08-21-072246.ips	23-Aug-22 10:05 AM	CA File	1 KB
Analytics-Journal-2022-08-22-072246.ips	23-Aug-22 10:05 AM	CA File	1 KB
Analytics-Journal-2022-08-23-073256.ips	23-Aug-22 10:05 AM	CA File	1 KB
forceReset-full-2022-08-18-150148	23-Aug-22 10:05 AM	IPS File	329 KB
JetsamEvent-2022-08-17-092907	23-Aug-22 10:05 AM	IPS File	63 KB
LowBatteryLog-2022-08-17-093911	23-Aug-22 10:05 AM	IPS File	2 KB

Elcomsoft အသုံးပြုပြီးရလာတဲ့ Crash Log File ဖြစ်ပါတယ်။

Libmobiledevice (Open Source)

Idevicecrashreport ဆိုတဲ့ Command ကိုအသုံးပြုပြီး Crash Log File ကိုရယူမှာဖြစ်ပါတယ်။ e = Extract ပြုလုပ်တာဖြစ်ပါတယ်။ , k = Crash Log ကို Device ကနေ မဖျက်ပဲရယူမှာဖြစ်ပါတယ်။ C:\SYS-LOG ကတော့ Crash Log ကိုသိမ်းထားမည့်နေရာဖြစ်ပါတယ်။ Libmobiledevice ကို Window မှာတင်မဟုတ်ပဲ Linux, Mac OS တွေမှာပါ အသုံးပြုနိုင်ပါတယ်။

Libmobiledevice Download

```
C:\>cd libimobiledevice-windows-master

C:\libimobiledevice-windows-master>idevicecrashreport.exe -e -k C:\SYS-LOG
Copy: /stacks+mediaserverd-2021-08-11-120919.ips
Copy: /Analytics-Journal-2022-08-22-072246.ips.ca
Copy: /Analytics-2022-08-20-072248.ips.ca
Copy: /ResetCounter-2022-08-22-142534.ips
Copy: /LowBatteryLog-2022-08-19-050648.ips
Copy: /stacks-2022-08-22-141650.ips
Copy: /Analytics-Journal-2022-08-23-073256.ips.ca
Copy: /forceReset-full-2022-08-18-150148.ips
Copy: /Analytics-2022-08-21-072246.ips.ca
Copy: /stacks-2022-08-18-153723.ips
Unable to open local file 'C:\SYS-LOG/WiFi/WiFiManager/wifi-buf-08-22-2022__16:13:39.311.log'. Skipping...
Unable to open local file 'C:\SYS-LOG/WiFi/WiFiManager/wifi-buf-08-22-2022__16:13:42.038.log'. Skipping...
Unable to open local file 'C:\SYS-LOG/WiFi/WiFiManager/wifi-buf-08-22-2022__16:13:37.875.log'. Skipping...
Copy: /JetsamEvent-2022-08-17-092907.ips
Copy: /stacks-2022-08-22-151917.ips
Copy: /com.apple.appstored/appstored.log
Copy: /stacks-2022-08-22-161333.ips
```

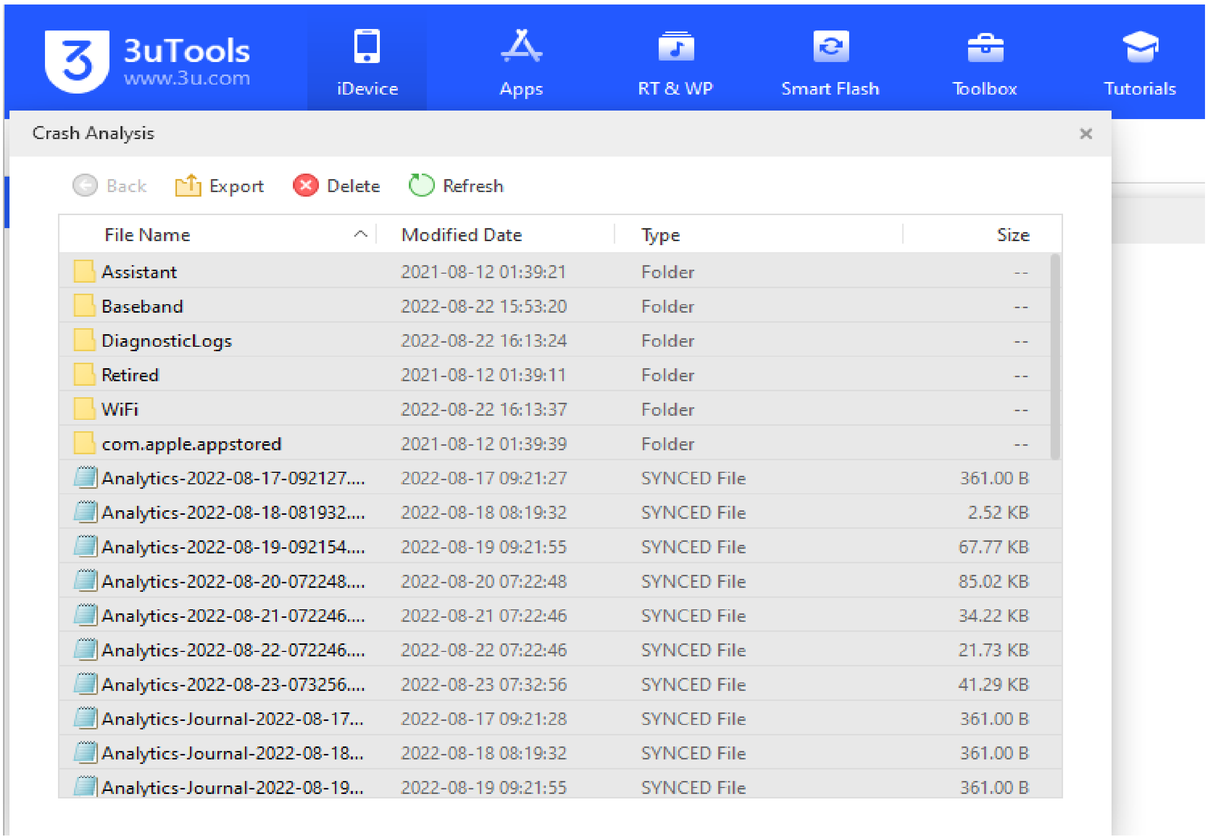
SYS-LOG › Search S

Name	Date modified	Type	Size
Assistant	23-Aug-22 10:01 AM	File folder	
Baseband	23-Aug-22 10:01 AM	File folder	
com.apple.appstored	23-Aug-22 10:01 AM	File folder	
DiagnosticLogs	23-Aug-22 10:01 AM	File folder	
Retired	23-Aug-22 10:01 AM	File folder	
WiFi	23-Aug-22 10:01 AM	File folder	
Analytics-2022-08-17-092127.ips	23-Aug-22 10:01 AM	CA File	1 KB
Analytics-2022-08-18-081932.ips	23-Aug-22 10:01 AM	CA File	3 KB
Analytics-2022-08-19-092154.ips	23-Aug-22 10:01 AM	CA File	68 KB
Analytics-2022-08-20-072248.ips	23-Aug-22 10:01 AM	CA File	86 KB
Analytics-2022-08-21-072246.ips	23-Aug-22 10:01 AM	CA File	35 KB
Analytics-2022-08-22-072246.ips	23-Aug-22 10:01 AM	CA File	22 KB
Analytics-2022-08-23-073256.ips	23-Aug-22 10:01 AM	CA File	42 KB
Analytics-Journal-2022-08-17-092128.ips	23-Aug-22 10:01 AM	CA File	1 KB
Analytics-Journal-2022-08-18-081932.ips	23-Aug-22 10:01 AM	CA File	1 KB
Analytics-Journal-2022-08-19-092155.ips	23-Aug-22 10:01 AM	CA File	1 KB
Analytics-Journal-2022-08-20-072248.ips	23-Aug-22 10:01 AM	CA File	1 KB
Analytics-Journal-2022-08-21-072246.ips	23-Aug-22 10:01 AM	CA File	1 KB
Analytics-Journal-2022-08-22-072246.ips	23-Aug-22 10:01 AM	CA File	1 KB
Analytics-Journal-2022-08-23-073256.ips	23-Aug-22 10:01 AM	CA File	1 KB
forceReset-full-2022-08-18-150148	23-Aug-22 10:01 AM	IPS File	329 KB
JetsamEvent-2022-08-17-092907	23-Aug-22 10:01 AM	IPS File	63 KB

Libmobiledevice အသုံပြုပြီးရလာတဲ့ Crash Log File ဖြစ်ပါတယ်။ Elcomsoft အသုံးပြုပြီးရယူယူတဲ့ ရလဒ်အတိုင်းပဲရရှိပါတယ်။

3UTools (Open Source)

3UTools Download



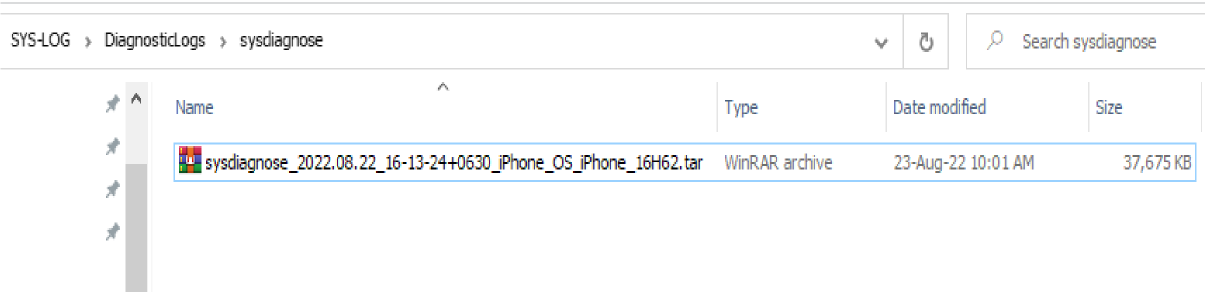
3UTools ကနေ Crash Log File ကို Export ပြုလုပ်နိုင်ပါတယ်။ အပေါ်မှာ အသုံးပြုတဲ့ Tools တွေကနေရရှိတဲ့ ရလဒ်အတိုင်းပဲရရှိမှာဖြစ်ပါတယ်။ 3UTools ကနေလဲ တစ်ခါတည်း Log File တွေကို ဖြည့်ကြည့်လို့ရပါတယ်။ Log File ကိုသိမ်းထားတဲ့နေရာကနေလဲ ကိုယ်လိုချင်တဲ့အပိုင်းကို ဖြည်ကြည့်လို့ရပါတယ်။ Elcomsoft IOS Forensics Tools Kit ကိုတော့ Log File တွေကိုဖြည်ကြည့်တဲ့နေရာ Analysis ပြုလုပ်တဲ့နေရာမှာ အသုံးပြုလို့မရပါဘူး။ Log File ကို Extraction ပြုလုပ်တဲ့နေရာမှာပဲ အသုံးပြု နိုင်ပါတယ်။ Open Source ကနေ Extraction ပြုလုပ်တဲ့ အခါရလာတဲ့ Log File အတိုင်းပဲ ရရှိမှာဖြစ်ပါတယ်။ Log File ကိုတော့ Text Editor နဲ့ အလွယ်တကူဖြည်ကြည့်နိုင်ပါတယ်။

Sysdiagnose

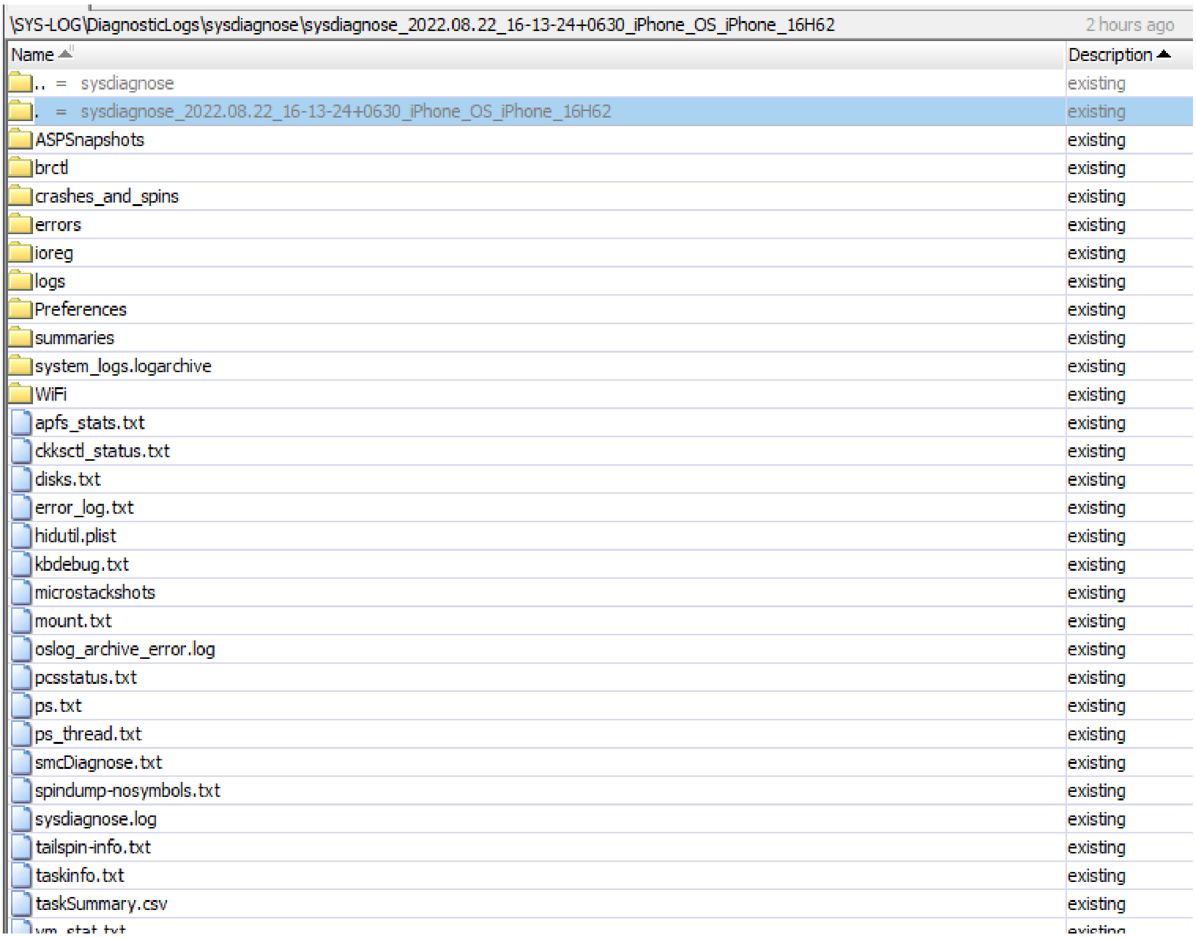
Sysdiagnose ကိုတော့ Bug Report အတွက် Developer တွေအသုံးပြုတာဖြစ်ပါတယ်။ Crash Log နဲ့မတူညီတဲ့အချက်တော့ System ကနေ Sysdiagnose Report ကို Automatic မထုတ်ပေးပါဘူး။ အသုံးပြုမယ်ဆိုရင် Manual ထုတ်ယူရမှာဖြစ်ပါတယ်။ AssitiveTouch ဒါမှမဟုတ် (Volume + Button နဲ့ Slide ဒါမှမဟုတ် Top Button ကို တစ်ပြိုင်ထဲ 1-1.5 Second နှိမ်ပြီးရယူနိုင်ပါတယ်။ Log File Size အပေါ်မူတည်ပြီး အချိန်အနည်းငယ်ကြာနိုင်ပါတယ်။ Sysdiagnose Log File Extension ကတော့ tar.gz ဖြစ်ပါတယ်။ Log File Location က Crash Logs Folder ရဲ့ DiagnosticLogs Folder အောက်ကို ရောက်သွားမှာဖြစ်ပါတယ်။ File Name မှာတော့ Sysdiagnose Log ကိုရယူတဲ့ အချိန် Device Type နဲ့ IOS Install Version ကိုတစ်ခါတည်းဖော်ပြထားပါတယ်။**(16H62 = IOS 12.5.5)**

တစ်ကယ်လို့ Apple Developer Account ရှိတယ်ဆိုရင် Log File တစ်ခုချင်းစီကို Device မှာ Profile သွင်းပြီး ရယူနိုင်ပါတယ်။ **See Detail**

iOS MacOS TvOS WatchOS တွေကနေလဲ Sysdiagnose ကိုရယူနိုင်ပါတယ်။



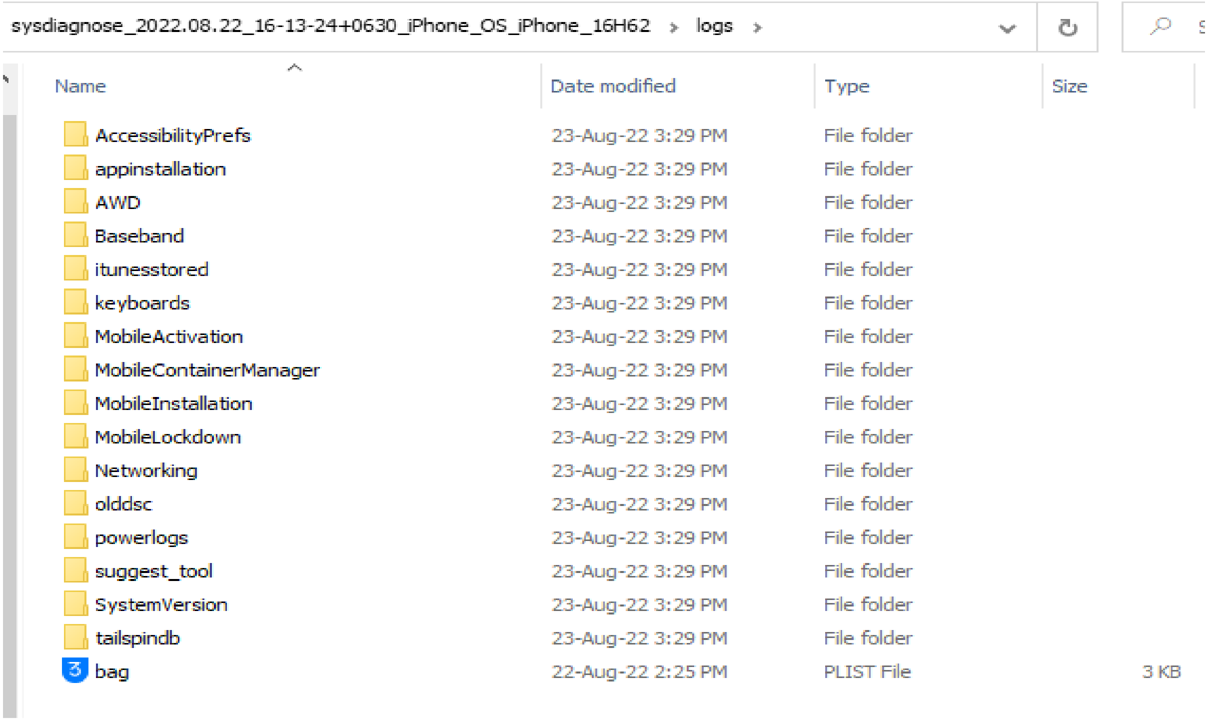
sysdiagnose_2022.08.22_16-13-24+0630_iPhone_OS_iPhone_16H62.tar


\SYS-LOG\DiagnosticLogs\sysdiagnose\sysdiagnose_2022.08.22_16-13-24+0630_iPhone_OS_iPhone_16H62 — 2 hours ago

Name	Description
.. = sysdiagnose	existing
. = sysdiagnose_2022.08.22_16-13-24+0630_iPhone_OS_iPhone_16H62	existing
ASPSnapshots	existing
brctl	existing
crashes_and_spins	existing
errors	existing
ioreg	existing
logs	existing
Preferences	existing
summaries	existing
system_logs.logarchive	existing
WiFi	existing
apfs_stats.txt	existing
ckksctl_status.txt	existing
disks.txt	existing
error_log.txt	existing
hidutil.plist	existing
kbdebug.txt	existing
microstackshots	existing
mount.txt	existing
oslog_archive_error.log	existing
pcsstatus.txt	existing
ps.txt	existing
ps_thread.txt	existing
smcDiagnose.txt	existing
spindump-nosymbols.txt	existing
sysdiagnose.log	existing
tailspin-info.txt	existing
taskinfo.txt	existing
taskSummary.csv	existing
vm_stat.txt	existing

Sysdiagnose ကိုဖြည်ကြည့်ရင်မြင်ရမဲ့ File တွေဖြစ်ပါတယ်။

Log Folder ကတော့ Forensics နဲ့ပတ်သတ်ပြီး အရေးကြီးတဲ့ Folder ဖြစ်ပါတယ်။ Configuration တွေ Log File တွေပါဝင်ပါတယ်။ IOS မည်သည့် Version ဖြစ်နေပါစေ Log Folder က Forensics Point Of View အတွက် အရေးပါပါတယ်။



Analysis လုပ်ဖို့အတွက် အောက်မှာဖော်ပြထားတဲ့ Open Source Tools တွေနဲ့ပြုလုပ်နိုင်ပါတယ်။

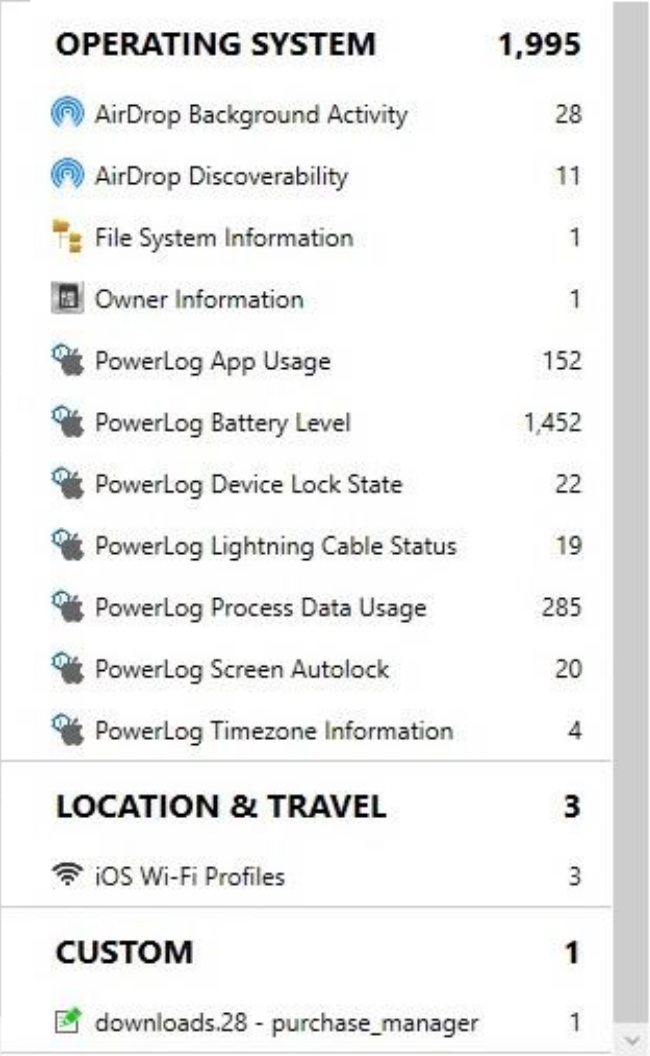
https://sqlitebrowser.org/dl/

https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts

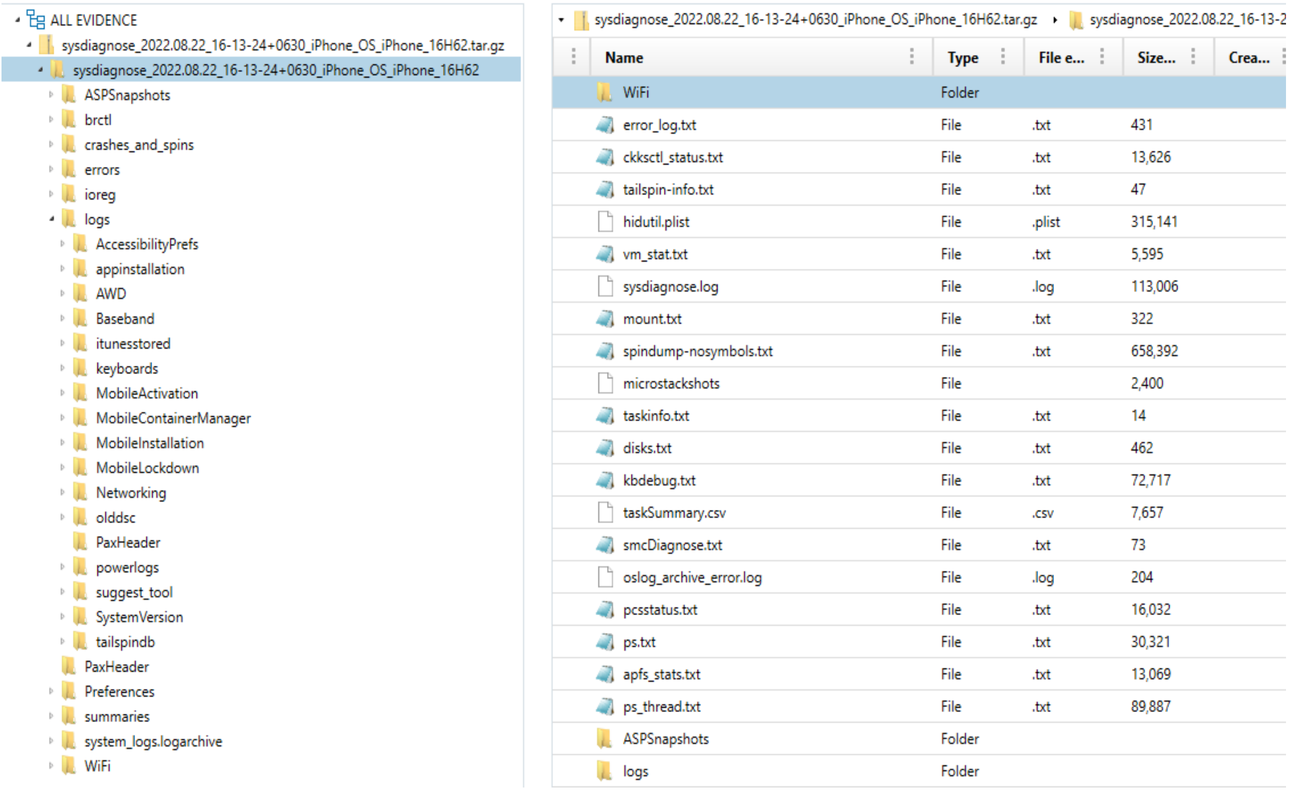
GitHub - abrignoni/iOS-Mobile-Installation-Logs-Parser

အခု PDF မှာတော့ Commercial Tools ဖြစ်တဲ့ Magnet Forensics Tools နဲ့ Sysdiagnose Log ကို Analysis ပြုလုပ်ထားပါတယ်။ Open Source Tools အချို့က Update အရမ်းမဖြစ်တဲ့အတွက်ဖြစ်ပါတယ်။ File System ကို Access မလုပ်ပဲနဲ့ Airdrop Record , Power Log Data, Application Permission, Mobile Application Log, Application Install State , Apple Contacts, Apple Maps Search, Installed Applications, Etc … စတာတွေကိုရှိနိုင်ပါတယ်။ Log ကနေရရှိမဲ့ Artifacts အနည်းအများကတော့ အသုံးပြုသူရဲ့ အလေ့အထနဲ့ သုံးစွဲမှုအပေါ် မူတည်ပြီးကွဲပြားနိုင်ပါတယ်။

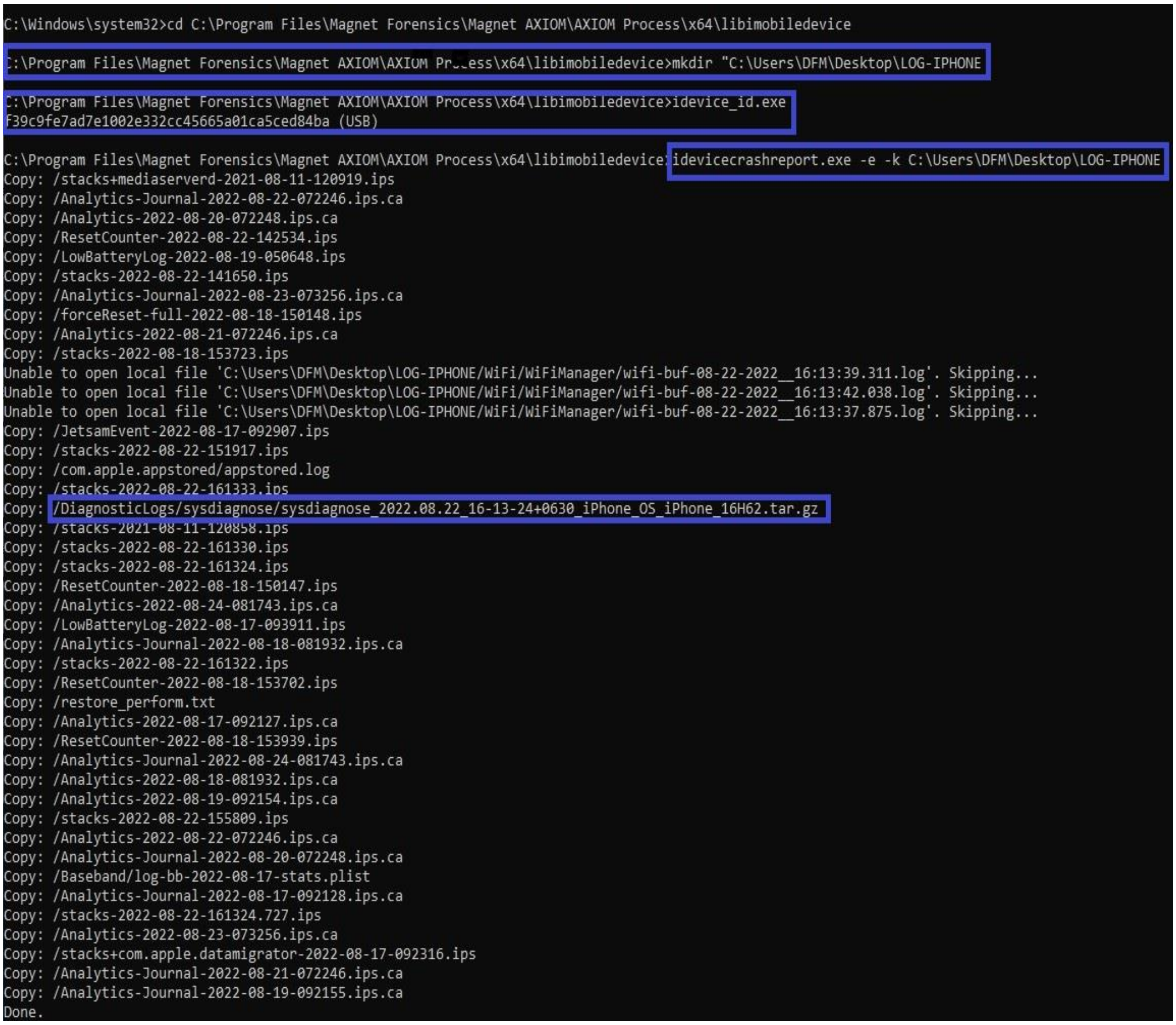
ALL EVIDENCE 2,663
REFINED RESULTS 9
Identifiers - Device 5
Identifiers - People 4
WEB RELATED 25
Potential Browser Activity 23
WebKit Browser Web History (Carved) 2
COMMUNICATION 1
MEDIA 4
AMR Files 1
Photoshop Files 3
EMAIL & CALENDAR 3
Apple Mail Fragments 3
DOCUMENTS 108
CSV Documents 2
Text Documents 106
APPLICATION USAGE 514
Application Install States 514


OPERATING SYSTEM 1,995
AirDrop Background Activity 28
AirDrop Discoverability 11
File System Information 1
Owner Information 1
PowerLog App Usage 152
PowerLog Battery Level 1,452
PowerLog Device Lock State 22
PowerLog Lightning Cable Status 19
PowerLog Process Data Usage 285
PowerLog Screen Autolock 20
PowerLog Timezone Information 4
LOCATION & TRAVEL 3
iOS Wi-Fi Profiles 3
CUSTOM 1
downloads.28 - purchase_manager 1

Sysdiagnose Log ကို Magnet ထဲကို ထည့်လိုက်တဲ့အခါမှာ ရလာတဲ့ Artifacts တွေဖြစ်ပါတယ်။



Sysdiagnose Log ကို Magnet ထဲမှာ File System View နဲ့လဲ Analysis ပြုလုပ်နိုင်ပါတယ်။



```
C:\Windows\system32>cd C:\Program Files\Magnet Forensics\Magnet AXIOM\AXIOM Process\x64\libimobiledevice

:\Program Files\Magnet Forensics\Magnet AXIOM\AXIOM Pr..ess\x64\libimobiledevice>mkdir "C:\Users\DFM\Desktop\LOG-IPHONE

:\Program Files\Magnet Forensics\Magnet AXIOM\AXIOM Process\x64\libimobiledevice>idevice_id.exe
f39c9fe7ad7e1002e332cc45665a01ca5ced84ba (USB)

C:\Program Files\Magnet Forensics\Magnet AXIOM\AXIOM Process\x64\libimobiledevice>idevicecrashreport.exe -e -k C:\Users\DFM\Desktop\LOG-IPHONE
Copy: /stacks+mediaserverd-2021-08-11-120919.ips
Copy: /Analytics-Journal-2022-08-22-072246.ips.ca
Copy: /Analytics-2022-08-20-072248.ips.ca
Copy: /ResetCounter-2022-08-22-142534.ips
Copy: /LowBatteryLog-2022-08-19-050648.ips
Copy: /stacks-2022-08-22-141650.ips
Copy: /Analytics-Journal-2022-08-23-073256.ips.ca
Copy: /forceReset-full-2022-08-18-150148.ips
Copy: /Analytics-2022-08-21-072246.ips.ca
Copy: /stacks-2022-08-18-153723.ips
Unable to open local file 'C:\Users\DFM\Desktop\LOG-IPHONE/WiFi/WiFiManager/wifi-buf-08-22-2022__16:13:39.311.log'. Skipping...
Unable to open local file 'C:\Users\DFM\Desktop\LOG-IPHONE/WiFi/WiFiManager/wifi-buf-08-22-2022__16:13:42.038.log'. Skipping...
Unable to open local file 'C:\Users\DFM\Desktop\LOG-IPHONE/WiFi/WiFiManager/wifi-buf-08-22-2022__16:13:37.875.log'. Skipping...
Copy: /JetsamEvent-2022-08-17-092907.ips
Copy: /stacks-2022-08-22-151917.ips
Copy: /com.apple.appstored/appstored.log
Copy: /stacks-2022-08-22-161333.ips
Copy: /DiagnosticLogs/sysdiagnose/sysdiagnose_2022.08.22_16-13-24+0630_iPhone_OS_iPhone_16H62.tar.gz
Copy: /stacks-2021-08-11-120858.ips
Copy: /stacks-2022-08-22-161330.ips
Copy: /stacks-2022-08-22-161324.ips
Copy: /ResetCounter-2022-08-18-150147.ips
Copy: /Analytics-2022-08-24-081743.ips.ca
Copy: /LowBatteryLog-2022-08-17-093911.ips
Copy: /Analytics-Journal-2022-08-18-081932.ips.ca
Copy: /stacks-2022-08-22-161322.ips
Copy: /ResetCounter-2022-08-18-153702.ips
Copy: /restore_perform.txt
Copy: /Analytics-2022-08-17-092127.ips.ca
Copy: /ResetCounter-2022-08-18-153939.ips
Copy: /Analytics-Journal-2022-08-24-081743.ips.ca
Copy: /Analytics-2022-08-18-081932.ips.ca
Copy: /Analytics-2022-08-19-092154.ips.ca
Copy: /stacks-2022-08-22-155809.ips
Copy: /Analytics-2022-08-22-072246.ips.ca
Copy: /Analytics-Journal-2022-08-20-072248.ips.ca
Copy: /Baseband/log-bb-2022-08-17-stats.plist
Copy: /Analytics-Journal-2022-08-17-092128.ips.ca
Copy: /stacks-2022-08-22-161324.727.ips
Copy: /Analytics-2022-08-23-073256.ips.ca
Copy: /stacks+com.apple.datamigrator-2022-08-17-092316.ips
Copy: /Analytics-Journal-2022-08-21-072246.ips.ca
Copy: /Analytics-Journal-2022-08-19-092155.ips.ca
Done.
```

Sysdiagnose Log ကို Magnet မှာပါတဲ့ libmobiledevice အသုံးပြုပြီးရယူတာ ဖြစ်ပါတယ်။

LOG-IPHONE >

Name	Date modified	Type	Size
Assistant	8/24/2022 9:05 AM	File folder	
Baseband	8/24/2022 9:05 AM	File folder	
com.apple.appstored	8/24/2022 9:04 AM	File folder	
DiagnosticLogs	8/24/2022 9:04 AM	File folder	
Retired	8/24/2022 9:05 AM	File folder	
WiFi	8/24/2022 9:04 AM	File folder	
Analytics-2022-08-17-092127.ips.ca	8/24/2022 9:05 AM	CA File	1 KB
Analytics-2022-08-18-081932.ips.ca	8/24/2022 9:05 AM	CA File	3 KB
Analytics-2022-08-19-092154.ips.ca	8/24/2022 9:05 AM	CA File	68 KB
Analytics-2022-08-20-072248.ips.ca	8/24/2022 9:04 AM	CA File	86 KB
Analytics-2022-08-21-072246.ips.ca	8/24/2022 9:04 AM	CA File	35 KB
Analytics-2022-08-22-072246.ips.ca	8/24/2022 9:05 AM	CA File	22 KB
Analytics-2022-08-23-073256.ips.ca	8/24/2022 9:05 AM	CA File	42 KB
Analytics-2022-08-24-081743.ips.ca	8/24/2022 9:05 AM	CA File	81 KB
Analytics-Journal-2022-08-17-092128.ips....	8/24/2022 9:05 AM	CA File	1 KB
Analytics-Journal-2022-08-18-081932.ips....	8/24/2022 9:05 AM	CA File	1 KB
Analytics-Journal-2022-08-19-092155.ips....	8/24/2022 9:05 AM	CA File	1 KB
Analytics-Journal-2022-08-20-072248.ips....	8/24/2022 9:05 AM	CA File	1 KB
Analytics-Journal-2022-08-21-072246.ips....	8/24/2022 9:05 AM	CA File	1 KB
Analytics-Journal-2022-08-22-072246.ips....	8/24/2022 9:04 AM	CA File	1 KB
Analytics-Journal-2022-08-23-073256.ips....	8/24/2022 9:04 AM	CA File	1 KB
Analytics-Journal-2022-08-24-081743.ips....	8/24/2022 9:05 AM	CA File	1 KB
forceReset-full-2022-08-18-150148	8/24/2022 9:04 AM	IPS File	329 KB
JetsamEvent-2022-08-17-092907	8/24/2022 9:04 AM	IPS File	63 KB
LowBatteryLog-2022-08-17-093911	8/24/2022 9:05 AM	IPS File	2 KB
LowBatteryLog-2022-08-19-050648	8/24/2022 9:04 AM	IPS File	1 KB
ResetCounter-2022-08-18-150147	8/24/2022 9:05 AM	IPS File	1 KB
ResetCounter-2022-08-18-153702	8/24/2022 9:05 AM	IPS File	1 KB
ResetCounter-2022-08-18-153939	8/24/2022 9:05 AM	IPS File	1 KB
ResetCounter-2022-08-22-142534	8/24/2022 9:04 AM	IPS File	1 KB

IOS Crash & Sysdiagnose Log တွေကိုရယူတာက IOS , macOS, Apple TV , Apple Watch တွေကနေရယူနိုင်ရုံသာမက Device Password မသိခဲ့ရင် ဒါမှမဟုတ် iCloud Active မဖြစ်ခဲ့ရင်တောင်မှ IOS Crash & Sysdiagnose Log တွေကိုရယူနိုင်ပါတယ်။ PDF မှာလဲ ICloud Log ကျနေတဲ့ Iphone ကနေ Log တွေကိုရယူထားတာဖြစ်ပါတယ်။ ဒါကြောင့် Result မှာ Artifacts နည်းနေတာဖြစ်ပါတယ်။

Commercial Version ဖြစ်တဲ့ Elcomsoft IOS Forensics , Magnet Axomi တွေမှာလဲ Apple Devices တွေကနေ Log တွေကို Extraction ရယူ တဲ့အခါမှာ အသုံးပြုတာက Open Source ဖြစ်တဲ့ libmobiledevice ပဲ ဖြစ်ပါတယ်။ ဒါကြောင့် Log Extraction ရယူတဲ့နေရာမှာ ရရှိလာတဲ့ Log File တွေမှာ Size ကအစ အကုန်တူညီ နေတာဖြစ် ပါတယ်။ IOS Update ထွက်တာနဲ့အမျှ Bug Error , Debug Error တွေအတွက် Log တွေအကြောင်းကို Apple မှာသွားရောက် လေ့လာနိုင်ပါတယ်။ တစ်ကယ်တန်းမှာ Developer တွေအတွက် ထုတ်ပေးတဲ့ Log တွေထဲကနေ Forensics အတွက် အသုံးဝင်နိုင်တဲ့ Log တွေကိုရယူတာဖြစ်ပါတယ်။